Version Number: 01-2017

U.S. Department of Commerce
Census Bureau

Privacy Impact Assessment
for the
Associate Director for Economic Programs
Innovation and Technology Office

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.21 17:32:31 -04'00' 02/04/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau CEN36 Applications

Unique Project Identifier: 006-00402100 00-07-01-02-01-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
CEN36 consists of several major applications that store PII/BII information such as name, address, business name, email address, telephone number etc.

Major applications that collect, maintain, process, and/or disseminate PII include:

Content Metadata System (COMET) - COMET is a major application for the long-term solution to standardize input requirements across modes of data collection including metadata across surveys and Census in support of dissemination. COMET does not store PII/BII.

Census Image Retrieval Application (CIRA) – CIRA contains the Decennial Data Capture Images as well as the edited and unedited data. This application is used by survey analysts to review anomalies in Data for specified tasks. This application has an extensive approval process in order for any individual to access or review data. Users only have access to view approved images and data based on an approved business case and are Census employee/contractors.

Integrated Computer Assisted Data Entry (iCADE) – The iCADE system scans and keys data from demographic, economic, and decennial census questionnaires received by mail from respondents. The iCADE reports module provides real-time status information for survey sponsors.

MOJO Optimizer – The MOJO Optimizer operational control system uses automation to support the scheduling, workload assignments, and management processes of field data collection efforts. It provides optimization of caseloads handled by enumerators through a Geographic Information System (GIS) to maximize productivity. MOJO allows authorized Census Bureau users to Browse Living Quarters (BLQ) data. The MOJO Hermes application generates management reports.

MOJO Recruiting Dashboard – The MOJO Recruiting Dashboard provides data to managers so they can monitor operations performance by providing insight into the progress of recruiting operations at lower levels of geography (tract).

(b) System location

COMET – hosted within the Census Bureau's Bowie Computer Center (BCC) located in Bowie, Maryland.

CIRA – hosted within the National Processing Center (NPC) in Jeffersonville, Indiana.

iCADE,- hosted in the following locations:

- National Processing Center (NPC) in Jeffersonville, Indiana
- Paper Data Capture Center-East in Jeffersonville, Indiana
- Paper Data Capture Center-West in Phoenix, Arizona

MOJO – hosted in the following locations:

- Census Bureau's Bowie Computer Center (BCC) in Bowie, Maryland
- AWS GovCloud (US-East) Region located in the Northeastern United States

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

COMET interconnects internally with iCADE to support the delivery of question content and metadata to create an iCADE master template for data capture scan testing and production processing. COMET (CEN36) interconnects with Centurion (CEN15) to provide metadata needed to render electronic instruments.

iCADE (CEN36) interconnects with the National Processing Center (NPC) (CEN06) to provide case status information to the Automated Tracking and Control System (ATAC). iCADE interconnects with the Enterprise Collection and Survey Enabling Platform (ECaSE) (CEN05) to pass paper response data and event data needed for ECaSE to perform sufficiency checks, and add post processing variables for subsequent processing by downstream systems. PEARSIS will deliver data from the Administrative Records T13 Composite file, which iCADE will use to improve the Optical Character Recognition (OCR) match rate.

MOJO receives contact strategy information from the Research & Methodologies Directorate and Non-Response Follow Up (NRFU) files from Decennial Census (CEN08). This strategy information includes respondent data from ECaSE and enumerator information from DAPPS. MOJO receives one-directional exchange of data from the Census Data Lake (CDL) in CEN18, which consists of Workload, Event, Paradata, Response, and Sample Delivery File (SDF) data for the Browse Living Quarters (BLQ) application.

CEN36 shares information with the following internal Census Bureau IT systems: CEN05 ECaSE, CEN06 National Processing Center (NPC) systems, CEN07 Geography, CEN08 Decennial, CEN15 Centurion, CEN18 CDL and CEN21 DAPPS.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
COMET – provides a repository for content metadata, a user interface for managing content, producing record layouts and data dictionaries, and creating and approving Office of Management and Budget (OMB) Pre-submission and Clearance Packages.

CIRA – provides a query browser that allows analysts to review data and its associated images for a specific, approved business case.

iCADE - receives paper questionnaires from respondents via the United States Postal Service (USPS) where the staff at the National Processing Center (NPC) opens the envelopes and removes the forms. The forms are scanned by iCADE scanner operators and respondent data is captured in an automated fashion with use of Optical Character Recognition (OCR) and Optical Mark Recognition (OMR). Any respondent data that is not captured via OMR or OCR is then sent to an iCADE keyer for capture. All respondent data is held in a script file and then transferred to the survey sponsor owner via a secured connection.

MOJO – receives enumerator information from Decennial Applicant, Personnel and Payroll System (DAPPS), contact strategy information from the Research & Methodologies Directorate, and Non-response follow-up (NRFU) workload from the Enterprise Collection and Survey Enabling Platform (ECaSE) system. MOJO will take the information and create daily workload assignments that will be pushed back to ECaSE. MOJO will also receive workload, event, ISR instrument paradata, response, and SDF for Census operations from the Census Data Lake (CDL).

(e) How information in the system is retrieved by the user
COMET – provides a software browser user interface for accessing questionnaire information contained within the repository. COMET will allow for assignment of user roles with unique permissions. These roles are either context independent (across various surveys) or context dependent (specific to a survey).

CIRA – provides a software browser user interface for reviewing data and associated images. User access to the images and supporting variables is strictly controlled. Requests for project approval and user access is on a case-by-case basis.

iCADE - provides a software user interface data capture solution for paper-based data collection operations, real-time reports on workflow, survey processing completeness, and accuracy and performance metrics for all automatic and clerical processes. It is only accessible to select users that have had their login credentials validated against the Census LDAP.

MOJO – The Optimizer application provides no end user access. Optimizer information within MOJO is accessed by system administrators via web services for the purpose of monitoring generation of workload assignments. The MOJO BLQ application will provide approved Area Census Office (ACO), Regional Census Office (RCC), and headquarters (HQ) staff the ability to search for housing units in the enumeration universe using the same protocols as currently deployed within the Recruiting Dashboard.

(f) How information is transmitted to and from the system
COMET – Information transmission to and from the COMET system is accomplished via Web Services using the COMET Service Registry in XML format. COMET also uses JSON to deliver data to Centurion, and has a direct DB link for iCADE.

CIRA – The Census Image Retrieval Application (CIRA) is limited to image searching and viewing. No data is transmitted to the end users. CIRA does not permit users to upload, modify or delete data or form images within the CIRA database.

iCADE – Information transmitted to and from iCADE is accomplished via secure protocols in XML format. Information output files for the sponsors can be created in a variety of formats including ASCII, EXCEL, TXT, and Oracle.dmp.

MOJO – Information transmitted to and from MOJO is accomplished via Java Database Connectivity (JDBC) and secure file transfer mechanisms.

(g) Any information sharing conducted by the system
The CEN36 applications only share PII and BII within other CEN36 applications and components and within other Census Bureau IT systems.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
15 U.S.C. 301.
13 U.S.C. Chapter 5, 6(c), 8(b), 131, 132, 141, 161, 182, 193, 196

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
The FIPS 199 rating for CEN36 systems is Moderate.

<u>Section 1</u>: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New MOJO application functionality; Recruiting Dashboard, BLQ and Hermes migrated to AWS GovCloud in 2018/2019.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

CEN36 major applications use a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to, data validation controls to ensure accuracy of information. It is the responsibility of the internal sponsor to vet system information for accuracy and transform it into a format that the external sponsor can ingest.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Census Bureau information shapes important policy and operational decisions that help improve the Nation's social and economic conditions. We conduct the constitutionally mandated Census of Population and Housing every ten years, which is used to apportion seats in the House of Representatives and informs congressional redistricting. The PII collected, maintained, and/or disseminated by CEN36 major applications is in reference to members of the public.

We also conduct a census of all business establishments and of all governmental units, known respectively as the Economic Census and the Census of Governments, every five years. The Economic Census is the benchmark used for measuring Gross Domestic Product (GDP) and other key indicators that guide public policy and business decisions.

In addition, we conduct several ongoing business and household surveys that provide the information in several of the Nation's key economic indicators and which is used to allocate over $400 billion in Federal funding annually.

The PII/BII collected for statistical purposes: The PII/BII maintained is from voluntary and mandatory surveys, census interviews, pilot tests and cognitive interviews collected from member of the public.

The PII collected for administrative purposes: CEN36 collects information about Census Bureau employees during the collection of respondent information. Field representative and interviewer characteristics obtained during census and survey interviews, pilot tests, and cognitive interviews are used for research and analytical studies to evaluate Census Bureau surveys and programs.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The census Bureau also deploys a Data Loss Prevention solution.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			

Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN05, CEN06, CEN07, CEN08, CEN15, CEN18, CEN21 CEN36 uses security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publications. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption for data at rest, and various physical controls at the Census Bureau facilities that house information technology systems. The Census Bureau also deploys an enterprise Data Loss Prevention (DLP) solution.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: Privacy Act statements are provided at the point of collection.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII.
X	No, individuals do not have an opportunity to decline to provide	Specify why not: For mandatory surveys or censuses, the respondent does not have an opportunity to decline.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII for some questions.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Some Census Bureau surveys are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: Privacy Act Statement upon login, letter, interview, or during data collection.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: If the Census Bureau contacts the respondent for an update then the respondent can provide the updated information. For some Census Bureau surveys, individuals have the opportunity to provide updates to PII data within the submitted survey or survey website.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For surveys covered under SORNs Census-4 and Census-5 there are no access & contest requirements since the data is collected for statistical purposes.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All systems are audited and monitored per U.S. Census Bureau Enterprise Audit procedures.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ____07/10/2019_____________ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan

	of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are approved by the Disclosure Review Board

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended.

<u>Section 9</u>: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). COMMERCE/CENSUS-2, Performance Measurement Records http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Demographic Survey Collection (Census Bureau Sampling Frame)- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4, Economic Survey Collection http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Programs http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html

	COMMERCE/CENSUS-7, Demographic Survey Collection (Non-Census Bureau Sampling Frame)- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html SORNS that cover data received from DAPPS: COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-1.html OPM/GOVT-5: Recruiting, Examining, and Placement Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-3-records-of-adverse-actions-performance-based-reductions-in-grade-and-removal-actions-and-terminations-of-probationers.pdf OPM/GOVT-7: Applicant Race, Sex, National Origin, and Disability Status Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-7-applicant-race-sex-national-origin-and-disability-status-records.pdf
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: N1-29-98-1 N1-029-05-2 N1-029-10-3 NC1-29-82-4 N1-029-10-4 NC1-29-82-4, Item 56 N1-29-92-1, Item D or 12c DAA-0029-2013-0004
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Data elements are not directly identifiable alone but may indirectly identify individuals
X	Quantity of PII	Provide explanation: Although a serious or substantial number of individuals would be affected by loss, theft, or compromise, the PII collected and maintained is non-sensitive which is unlikely to result in harm to individuals.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, have little relevance outside the context.
X	Context of Use	Provide explanation: Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.
X	Access to and Location of PII	Provide explanation: The PII/BII is located on computers (including laptops) and networks, and IT systems controlled by the Census Bureau. Access is limited to those with a need to know including the Census Bureau geographic program area, regional offices, and survey program offices, etc.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As new people and configurations of systems come on board to process the 2020 Census, the threat from new employee error or intent is a potential threat. The necessity of scaling up to meet the rigors and demands in a tight economic environment with a reduced pool of potential employees makes staffing a particular challenge. Continued training and risk of legal enforcement mitigate for the threat.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.